**Scenario 1: Ransomware Attack Simulation**

**Overview:**

A ransomware attack is simulated on a financial services company. The goal is to demonstrate how the attack progresses through various stages, and how the Bayesian network representation can help in understanding and mitigating the threat.

**Steps:**

1. **Initial Access**:
   * **Technique**: Spearphishing Attachment (T1566.001)
   * **Description**: An employee receives an email with a malicious attachment that, when opened, grants the attacker initial access to the network.
2. **Execution**:
   * **Technique**: PowerShell (T1059.001)
   * **Description**: The malicious attachment runs a PowerShell script that downloads additional malware onto the compromised machine.
3. **Persistence**:
   * **Technique**: Scheduled Task/Job (T1053.005)
   * **Description**: The malware creates a scheduled task to ensure it runs every time the system boots.
4. **Privilege Escalation**:
   * **Technique**: Exploitation for Privilege Escalation (T1068)
   * **Description**: The malware exploits a vulnerability to gain higher privileges on the system.
5. **Defense Evasion**:
   * **Technique**: Obfuscated Files or Information (T1027)
   * **Description**: The malware obfuscates its files and communication to avoid detection by security tools.
6. **Credential Access**:
   * **Technique**: Credential Dumping (T1003)
   * **Description**: The malware dumps credentials from memory, the registry, or other storage locations.
7. **Discovery**:
   * **Technique**: System Network Configuration Discovery (T1016)
   * **Description**: The malware discovers network configuration and connected devices.
8. **Lateral Movement**:
   * **Technique**: Remote Services (T1021)
   * **Description**: The malware uses remote services to move laterally across the network.
9. **Collection**:
   * **Technique**: Data Staged (T1074)
   * **Description**: The malware collects and stages sensitive data for exfiltration.
10. **Exfiltration**:
    * **Technique**: Exfiltration Over Command and Control Channel (T1041)
    * **Description**: The malware exfiltrates data over an encrypted C2 channel.
11. **Impact**:
    * **Technique**: Data Encrypted for Impact (T1486)
    * **Description**: The malware encrypts critical files and demands a ransom for the decryption key.

**Scenario 2: APT Attack Combination(intellectual property theft and financial data breach)**

**Techniques for Intellectual Property Theft (IPT):**

1. **Initial Access**:
   * **Phishing (T1566)**: Score 1
   * **Valid Accounts (T1078)**: Score 3
2. **Execution**:
   * **User Execution (T1204)**: Score 1
3. **Persistence**:
   * **Valid Accounts (T1078)**: Score 3
4. **Credential Access**:
   * **OS Credential Dumping (T1003)**: Score 3
5. **Lateral Movement**:
   * **Remote Services (T1021)**: Score 3
6. **Collection**:
   * **Data from Information Repositories (T1213)**: Score 1

**Techniques for Financial Data Breach (FDB):**

1. **Initial Access**:
   * **External Remote Services (T1133)**: Score 2
   * **Valid Accounts (T1078)**: Score 3
2. **Execution**:
   * **Scripting (T1059)**: Score 2
3. **Persistence**:
   * **Valid Accounts (T1078)**: Score 3
4. **Credential Access**:
   * **OS Credential Dumping (T1003)**: Score 3
5. **Lateral Movement**:
   * **Remote Services (T1021)**: Score 3
6. **Exfiltration**:
   * **Exfiltration Over C2 Channel (T1041)**: Score 3
7. **Discovery**:
   * **System Network Configuration Discovery (T1016)**: Score 2

**Overlapping Techniques**

1. **Valid Accounts (T1078)**:
   * Tactics: Initial Access, Persistence, Privilege Escalation, Defense Evasion
   * Score: 3
2. **OS Credential Dumping (T1003)**:
   * Tactic: Credential Access
   * Score: 3
3. **Remote Services (T1021)**:
   * Tactic: Lateral Movement
   * Score: 3
4. **User Execution (T1204)**:
   * Tactic: Execution
   * Score: 1
5. **Phishing (T1566)**:
   * Tactic: Initial Access
   * Score: 1